

C.A. No. 09-10139

D. Ct. No. CR 07-1207-TUC-RCC

**UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

v.

HOWARD WESLEY COTTERMAN,

Defendant-Appellee.

ON APPEAL FROM A JUDGMENT OF THE UNITED STATES
DISTRICT COURT FOR THE DISTRICT OF ARIZONA

OPENING BRIEF OF APPELLANT

JOHN J. TUCHI
United States Attorney
District of Arizona

CHRISTINA M. CABANILLAS
Appellate Chief

CARMEN F. CORBIN
Assistant U.S. Attorney
405 West Congress, Suite 4800
Tucson, Arizona 85701
Telephone: (520) 620-7300
Attorneys for Appellant

Date Electronically Filed: August 31, 2009

I. TABLE OF CONTENTS

	Page
I. Table of Contents	i
II. Table of Authorities	ii
III. Statement of Jurisdiction	
A. District Court Jurisdiction	1
B. Appellate Court Jurisdiction	1
C. Timeliness of Appeal	1
D. Bail Status	1
IV. Issue Presented	2
V. Statement of the Case	
A. Nature of the Case; Course of Proceedings	4
B. Statement of Facts	5
VI. Summary of Argument	14
VII. Argument	
The District Court Erred When It Suppressed The Child Pornography Evidence Found On The Defendant's Laptop Computer	15
VIII. Conclusion	47
IX. Statement of Related Cases	48
X. Certificate of Compliance	49
XI. Certificate of Service	50

II. TABLE OF AUTHORITIES

CASES

<i>Alexander v. United States</i> , 362 F.2d 379 (9th Cir. 1966)	17, 36
<i>Almeida-Sanchez v. United States</i> , 413 U.S. 266 (1973)	19
<i>Carroll v. United States</i> , 267 U.S. 132 (1925)	16
<i>Torres v. Puerto Rico</i> , 442 U.S. 465 (1979)	16
<i>United States v. Abbouchi</i> , 502 F.3d 850 (9th Cir. 2007)	40
<i>United States v. Alfonso</i> , 759 F.2d 728 (9th Cir. 1985)	16, 17, 20, 27, 34, 37-39
<i>United States v. Arnold</i> , 523 F.3d 941 (9th Cir. 2008)	3, 15, 21, 28, 29, 37, 39
<i>United States v. Bareno-Burgos</i> , 739 F.Supp. 772 (E.D.N.Y. 1990)	41
<i>United States v. Bennett</i> , 363 F.3d 947 (9th Cir. 2004)	34
<i>United States v. Bennett</i> , 363 F.3d 947 (9th Cir. 2004)	3
<i>United States v. Bilir</i> , 592 F.2d 735 (4th Cir. 1979)	36, 39

<i>United States v. Burnette</i> , 698 F.2d 1038 (9th Cir. 1983)	22
<i>United States v. Caicedo-Guarnizo</i> , 723 F.2d 1420 (9th Cir. 1984)	19, 34
<i>United States v. Caminos</i> , 770 F.2d 361 (3d Cir. 1985)	32, 33, 36, 38
<i>United States v. Cardona</i> , 769 F.2d 625 (9th Cir. 1985)	15, 19, 20, 37, 40, 41
<i>United States v. Duncan</i> , 693 F.2d 971 (9th Cir. 1982)	26
<i>United States v. Espericueta-Reyes</i> 631 F.2d 616, 620 & n.4 (9th Cir. 1980)	35, 37
<i>United States v. Flores-Montano</i> , 541 U.S. 149 (2004)	17, 21, 37
<i>United States v. Gallagher</i> , 557 F.2d 1041 (4th Cir. 1977)	32, 33
<i>United States v. Gaviria</i> , 805 F.2d 1108 (2d Cir. 1986)	32, 33
<i>United States v. Guadalupe-Garza</i> , 421 F.2d 876 (9th Cir. 1970)	26
<i>United States v. Guzman-Padilla</i> , No. 08-50114 and No. 08-50118, 2009 WL 2182818 (9th Cir. July 23, 2009) .	3, 19
<i>United States v. Hill</i> , 459 F.3d 966 (9th Cir. 2006)	23-26, 42

<i>United States v. Ickes</i> , 2004 WL 5200395 (4th Cir. April 2, 2004)	29
<i>United States v. Ickes</i> , 393 F.3d 501 (4th Cir. 2005)	16, 18, 28, 29
<i>United States v. Mendenhall</i> , 446 U.S. 544 (1980)	19
<i>United States v. Mitchell</i> , 2007 WL 2915889 (S.D. Ga. 2007)	43
<i>United States v. Montoya de Hernandez</i> , 473 U.S. 532 (1985)	3, 15, 18, 19, 44
<i>United States v. Payton</i> , No. 07-10567, 2009 WL 2151348 (9th Cir. July 21, 2009)	21
<i>United States v. Ramsey</i> , 431 U.S. 606 (1977)	18
<i>United States v. Richards</i> , 638 F.2d 765 (5th Cir. 1981)	36
<i>United States v. Roberts</i> , 274 F.3d 1007 (5th Cir. 2001)	28, 30
<i>United States v. Romm</i> , 455 F.3d 990 (9th Cir. 2006)	28, 30
<i>United States v. Sahanaja</i> , 430 F.3d 1049 (9th Cir. 2005)	40
<i>United States v. Sheikh</i> , 654 F.2d 1057 (5th Cir. 1981)	32, 33

<i>United States v. Smith</i> , 629 F.2d 1301 (9th Cir. 1980)	31
<i>United States v. Thirty Seven Photographs</i> , 402 U.S. 363 (1971)	19
<i>United States v. Udofot</i> , 711 F.2d 831 (8th Cir. 1983)	41
<i>United States v. Weil</i> , 432 F.2d 1320 (9th Cir. 1970)	35
<i>United States v. Whiting</i> , 781 F.2d 692 (9th Cir. 1986)	20, 39
<i>United States v. Yang</i> , 286 F.3d 940 (7th Cir. 2002)	19, 44
<i>United States v. Zuniga-Salinas</i> , 952 F.2d 876 (5th Cir. 1992)	32

STATUTES

6 U.S.C. § 203	16
6 U.S.C. § 211	16
18 U.S.C. § 1073	4
18 U.S.C. § 1462(a)	4
18 U.S.C. § 1465	4
18 U.S.C. § 2251(a)	4
18 U.S.C. § 2251(e)	4

18 U.S.C. § 2252(a)(1)	4
18 U.S.C. § 2252(a)(4)(B)	4
18 U.S.C. § 2252(b)(1)	4
18 U.S.C. § 2252(b)(2)	4
18 U.S.C. § 2256(2)	4
18 U.S.C. § 3231	1
18 U.S.C. § 3509(c)	10
18 U.S.C. § 3731	1
19 C.F.R. § 162.6	17
19 U.S.C. § 482	16, 17, 43
19 U.S.C. § 1305	17
19 U.S.C. § 1496	17
19 U.S.C. § 1499(a)	17
19 U.S.C. § 1499(a)(1)	17
19 U.S.C. § 1499(a)(2)(B) and (b)	18
19 U.S.C. § 1499(b)	18
19 U.S.C. § 1499(c)(1)	18
19 U.S.C. § 1499(c)(5)(A)	18

19 U.S.C. § 1514(a)(4)	18
19 U.S.C. § 1581	17, 43
19 U.S.C. § 1582	17
19 U.S.C. § 1595a(c)(3)	17
22 U.S.C. § 464	17
50 App. U.S.C. § 2411(a)(2)(A)	17

RULES

Fed. R. App. P. 4(b)	1
----------------------------	---

III. STATEMENT OF JURISDICTION

A. District Court Jurisdiction

The district court had subject matter jurisdiction pursuant to 18 U.S.C. § 3231 because the defendant/appellant, Howard Cotterman (“the defendant”), was charged with a federal crime. (CR 9; ER 264-69.)¹

B. Appellate Court Jurisdiction

The United States, with Solicitor General approval, is appealing the district court’s order suppressing evidence discovered on the defendant’s laptop computer. (CR 71, 72; ER 1-2, 17-18.) This Court possesses jurisdiction over the government’s interlocutory appeal pursuant to 18 U.S.C. § 3731.

C. Timeliness of Appeal

Following the district court’s entry of its suppression order on February 23, 2009, the government filed a notice of appeal on March 19, 2009. (CR 72; ER 17-18.) The notice was timely pursuant to Fed. R. App. P. 4(b).

D. Bail Status

The defendant is currently in custody.

¹ “CR” refers to the Clerk’s Record and will be followed by pertinent document number(s). “RT” refers to the Reporter’s Transcript and will be followed by a date and relevant page number(s). “ER” refers to the Excerpts of Record and will be followed by relevant page number(s).

IV. ISSUE PRESENTED

WHETHER THE AUTHORITY TO SEARCH A LAPTOP COMPUTER WITHOUT REASONABLE SUSPICION AT A BORDER POINT OF ENTRY PERMITS LAW ENFORCEMENT TO TAKE IT TO ANOTHER LOCATION TO BE FORENSICALLY EXAMINED, WHEN IT HAS REMAINED IN THE CONTINUOUS CUSTODY OF THE GOVERNMENT.

V. STATEMENT OF THE CASE

The district court erred when it suppressed the child pornography evidence lawfully seized from the defendant's laptop computer during a border search. Routine searches of travelers and their belongings at an international border "are not subject to any requirement of reasonable suspicion, probable cause or warrant" *United States v. Montoya de Hernandez*, 473 U.S. 532, 538 (1985); *see United States v. Arnold*, 523 F.3d 941, 945-946 (9th Cir. 2008) (Fourth Amendment does not bar suspicionless search of contents of laptop computer at the border). However, reasonable suspicion is required for "extended border searches," which "occur after the actual entry has been effected" and "away from the border where entry is not apparent." *United States v. Guzman-Padilla*, No. 08-50114 and No. 08-50118, 2009 WL 2182818, at *4-*5 (9th Cir. July 23, 2009) (internal quotations omitted).

The district court concluded that, although agents lawfully seized the defendant's laptop at the border and checked his computer files briefly there, a forensic analyst's search of the detained laptop forty-eight hours later at a field office away from the border was an "extended border search" that required reasonable suspicion. However, unlike an extended border search, which occurs "after an actual entry and therefore intrude[s] more on an individual's normal expectation of privacy," *United States v. Bennett*, 363 F.3d 947, 951 (9th Cir. 2004), the analyst's examination

of the defendant's laptop was a continuation of the search initiated at the border and therefore did not implicate any heightened expectation of privacy. The laptop was never cleared through Customs between the time it was seized at the border and the forensic examination in Tucson, so it was still a border search. Requiring agents to search laptops and other electronic media at the time and place of entry could hamper the government's ability to conduct effective border searches. The laptop was lawfully searched and the district court's order should be reversed.

A. Nature of the Case; Course of Proceedings.

On June 27, 2007, a Tucson, Arizona grand jury charged the defendant in an indictment with various child pornography offenses. (CR 9; ER 264-69.) He was charged with: two counts of production of child pornography, in violation of 18 U.S.C. §§ 2251(a),(e) and 2256(2); transportation and shipping, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a)(4)(B), (b)(2) and 2256(2); importation and transportation of obscene material, in violation of 18 U.S.C. §§ 1462(a), 1465, 2252(a)(1),(2) and (b)(1); and flight to avoid prosecution, in violation of 18 U.S.C. § 1073.

Significant portions of the evidence were obtained through a search of the defendant's laptop computer that was seized at the Lukeville, Arizona Port of Entry (POE) at the U.S./Mexico border. The defendant filed a motion to suppress evidence

seized from his computer. (CR 17; ER 252-63.) After hearing evidence and argument, the district court granted the defendant's motion to suppress, finding that the search was an "extended border" search that required reasonable suspicion, and that reasonable suspicion was lacking here. (CR 58, 71; ER 3-16, 1-2.)

B. Statement of Facts

1. Events at the Port of Entry

At approximately 10:00 a.m. on Friday, April 6, 2007, the defendant, Howard Cotterman, a United States citizen, and his wife, Maureen Cotterman, applied for admission into the United States from the Republic of Mexico at the Lukeville POE in Arizona. (CR 58; ER 3.) The defendant and his wife arrived at primary inspection in their personal vehicle. Customs and Border Protection (CBP) Officers referred the Cottermans to secondary inspection based on information they received from an intelligence unit that targets convicted and registered sex offenders who travel abroad regularly. (CR 55; RT 8/27/08 11-12; ER 64-65; Resp. to Mot. to Supp. 1-2.)²

While at secondary inspection, record checks confirmed that the defendant had been convicted on February 25, 1992, in the Superior Court of California, of two counts of use of a minor in sexual conduct, two counts of lewd and lascivious conduct

²Because the government's response to the defendant's motion to suppress is still under seal below, it has been submitted under seal with this Court.

upon a child, and three counts of “child molest-inhabited dwelling,” all in violation of California Penal Codes. (Resp. to Mot. to Supp. 2; CR 28; ER 249-51.)

A search at secondary inspection revealed that the defendant and his wife possessed two Dell laptop computers, a Pentax Optio digital camera, a SONY video camera, and a Fuji Film E510 camera. (CR 58; ER 4; Resp. to Mot. to Supp. 2.) A preliminary search of one of the Dell laptop computers by CBP Officer Alvarado revealed that several files were password protected. (CR 58; ER 4.) The Immigration and Customs Enforcement (ICE) duty agent was notified and responded to investigate further. (*Id.*)

The defendant and his wife left the Lukeville POE late in the afternoon on April 6, 2007. (CR 58; ER 4.) The video camera and Fuji camera were reviewed and released to them before their departure. (Resp. to Mot. to Supp. 3.) Both Dell laptops and the Pentax digital camera were retained for forensic examinations at 6:00 pm on April 6, 2009. (CR 58; ER 4.)

2. Transportation & Examination of the Laptops in Tucson

Acting Resident Agent in Charge Craig Brisbane transported the items from the Lukeville POE to the ICE Office in Tucson. (CR 55; RT 8/27/08 17 ; ER 70; Resp. to Mot. to Supp. 3.) Brisbane delivered the items to Senior Special Agent and Computer Forensic Examiner John Owen at the ICE office in Tucson at approximately

10:00 p.m. that same day. (*Id.*) Owen checked the items into evidence and began his forensic examination the next day, Saturday, April 7, 2007. (*Id.*)

Over the course of the weekend, there was repeated telephonic contact between ICE agents and the Cottermans about the status of the examinations. (CR 55; RT 8/27/08 18-20; ER 71-73; Resp. to Mot. to Supp. 4.) On Saturday, the forensics examination of the Pentax Optio digital camera was completed with negative results. The Cottermans responded to the ICE office in Tucson on Saturday afternoon, and the defendant signed the property receipt form and took possession of the digital camera. The forensic examinations were still in progress on the Dell laptop computers at that time, so they were not released. (CR 55; RT 8/27/08 18-20; ER 71-73.)

On Sunday, April 8, 2007, the forensic examination of the Dell laptop computer belonging to the defendant, an Inspiron 8600 with Serial Number 5VJ0T61, resulted in the discovery of approximately 75 child pornographic images in unallocated clusters. (CR 58; ER 4; Resp. to Mot. to Supp. 4.) There were also numerous password-protected .zip files in folders on that same hard drive. (Resp. to Mot. to Supp. 4.)³

³The laptop belonging to Mrs. Cotterman, a Dell Inspiron 8600 with Serial Number D2K0T61, did not contain any child pornography.

ICE agents contacted the defendant on his cell phone and asked him to come to the ICE office the next day, on Monday, April 9, 2007, at 9:30 a.m., to assist the forensics examiner in completing the examination to return his laptop to him. (Resp. to Mot. to Supp. 4.) Agents did not mention the images of child pornography that had been discovered. The defendant agreed to come to the office on Monday morning.

3. Defendant's Flight from the United States

On Monday, however, the defendant did not appear. (CR 55; RT 8/27/08 20-21; ER 73-74; Resp. to Mot. to Supp. 4.) Instead, Mrs. Cotterman arrived at the ICE office that morning and her laptop was returned to her. Unbeknownst to agents at the time, the defendant boarded an Aeromexico flight on Monday from Tucson to Hermosillo, Mexico. (CR 55; RT 8/27/08 22; ER 75.) His intended destination was Sydney, Australia, via Ciudad Juarez, Vancouver and Tokyo. (CR 58; ER 5; Resp. to Mot. to Supp. 5.) When his travel itinerary became known, law enforcement notified the ICE Attaché in Singapore in an effort to have Cotterman denied entry into Australia and repatriated to the United States. (Resp. to Mot. to Supp. 5.) However, Cotterman was able to successfully make entry at Sydney International Airport on the morning of April 12, 2007. (*Id.*)

4. Further Examination of the Laptop & Discovery of More Child Pornography

After the defendant fled the country on April 9, 2007, Owen continued his forensic examination. (*Id.*) On April 11, 2007, he was able to access the 23 password protected .zip files on one of the hard drives on Cotterman's computer. He found approximately 378 images and eleven video files of child pornography. (*Id.*) Approximately 360 of the 378 images of child pornography and all eleven videos depicted the same nude or partially nude female, approximately seven to ten years old, engaged in various sexual acts. (*Id.*) In a number of the images, an older man, who appeared to be the defendant, was touching and manipulating the minor female's genitals and pubic area. Further analysis revealed the presence of an additional 1206 images of child pornography on the same hard drive, as well as approximately 309 stories of sexual abuse and acts of incest involving minors. (Resp. to Mot. to Supp. 5-6.)

Agents discovered ten CDs that were left at the Lukeville POE, located shortly after the Cottermans' departure on April 6, 2007. They were held at the DHS-CBP/ICE office in Lukeville. (Resp. to Mot. to Supp. 6.) These items were forwarded to Agent Mina Riley at the ICE office in Sells in July 2007, and then given to Owen at the Tucson ICE office to forensically examine in August 2007. During his

examination of those items, Owen located a number of child pornography files saved to one CD. This CD appears to be a back-up copy of many of the files located on the defendant's laptop.

5. California Search Warrant

On or about April 13, 2007, a search warrant was executed at the defendant's residence in Truckee, California. (Resp. to Mot. to Supp. 6.) A number of items, including 415 CDs, 202 3.5" floppy diskettes, zip disks, back-up tapes and a number of computers were seized. Examination of those items has revealed over 330 images and eighteen videos of child pornography that appeared to involve the same victim being abused by the defendant.⁴

6. Discovery of the Victim & Defendant's Extradition from Australia

On April 25, 2007, U.S. law enforcement authorities identified and interviewed the minor female victim being abused in the images and videos. (Resp. to Mot. to Supp. 6-7.)⁵

⁴The Eastern District of California has indicted the defendant with multiple offenses in United States v. Cotterman, CR 07-0484-GEB.

⁵Further discussion of the minor victim's and her mother's statements to law enforcement are contained in the government's response to the motion to suppress. The government asked that the document be filed under seal below, pursuant to 18 U.S.C. § 3509(c). It remains under seal and has been provided to this Court under
(continued...)

On September 8, 2007, Australian law enforcement authorities arrested the defendant in Coffs Harbour, Australia, pursuant to a United States provisional arrest warrant. (Resp. to Mot. to Supp. 7.) The defendant was then extradited to Arizona.

7. Pending Charges

On June 27, 2007, a grand jury in Tucson, Arizona returned an indictment charging the defendant with various offenses, as set forth earlier. (CR 9; ER 264-69.) The indictment also seeks forfeiture of the defendant's laptop and two hard drives. The defendant made his initial appearance on the Arizona charges in Tucson on March 31, 2008. His detention hearing was held on April 3, 2008, at which time he was ordered detained. (CR 16.)

8. Motion to Suppress Evidence

On April 18, 2008, the defendant filed a motion to suppress evidence and a request for an evidentiary hearing. (CR 17; ER 252-63.) He claimed that the initial border search, the seizure of the laptop without particularized suspicion, and the subsequent forensic analysis without a warrant were unreasonable. He asked the court to suppress the evidence discovered from his laptop, as well as any fruits of that search. The government filed a response, arguing that the laptop was lawfully

⁵(...continued)
seal.

searched during a border search. (Resp. to Mot. to Supp.) A hearing was conducted before a magistrate on August 27, 2008. (CR 55; ER 54-218.)

9. Magistrate's Report and Recommendation and District Court's Ruling

On September 12, 2008, the magistrate issued a Report and Recommendation (R & R), recommending that the district court grant the defendant's motion to suppress the evidence found on his laptop computer. It found that the search of the defendant's laptop became an "extended border search" because the forensic analysis occurred away from the initial point of entry into the United States, and therefore, it needed to be supported by reasonable suspicion. The magistrate stated:

In this case, the first evidence of child pornography was discovered 170 miles from the Lukeville port of entry, and at least two days afer (sic) the Cottermans entered the United States Under those circumstances, the law requires the Government to have reasonable suspicion before extending the search in both distance and time away from the border.

(CR 58; ER 8.) The court also found that reasonable suspicion was lacking. (CR 58; ER 8, 13, 15.) It also ordered the return of a government hard drive and photocopies of paperwork, relief that was not requested by the defendant. (CR 58; ER 13, 16.)⁶

On February 23, 2009, the district court adopted that recommendation. (CR 71; ER 1-2.) Based on the time the Cottermans waited at the border (8 hours), the time

⁶ The government had also argued that the defendant abandoned the laptop (Resp. to Mot. to Supp. 14-15), but the magistrate disagreed. (CR 58; ER 13-15.)

it took Owen to search the defendant's laptop (48 hours), the geographical distance from the actual border where the search took place (170 miles), and the fact that it found that "the technician could have traveled down from Tucson with his laptop to do the analysis," the district court categorized the search as an "extended border search," rather than a search at the border or its functional equivalent. (CR 71; ER 1-2.) The district court agreed with the magistrate that reasonable suspicion was required and found that such reasonable suspicion was not present in this case. (CR 71; ER 1-2.)

The district granted the defendant's motion to suppress, ordered the government to return Mrs. Cotterman's computer and retain no copy of it, and ordered the return of the "Cottermans['] personal papers that were photocopied at the border and retain no copies." (CR 71; ER 1-2.)⁷

The government, with Solicitor General approval, now appeals the suppression order.

⁷ Not only did the district court suppress evidence obtained from the defendant's computer and other items mentioned above, but its suppression order also appears to encompass the CDs found at the Lukeville POE, because the magistrate stated that the CDs were not "abandoned" for Fourth Amendment purposes. (CR 71; ER 1-2.)

VI. SUMMARY OF ARGUMENT

The district court erred by suppressing the evidence discovered on the defendant's laptop computer. The forensic examination of the computer constituted a border search, even though it occurred a distance from the border, because the computer was never cleared by Customs to enter the United States and remained in their custody. The examination of the laptop was a continuation of the search initiated at the border and therefore did not implicate any heightened expectation of privacy. A contrary rule requiring agents to search laptops and other electronic media at the time and place of entry could hamper the government's ability to conduct effective border searches. The district court erroneously determined that the search of the defendant's laptop was an "extended border search" requiring reasonable suspicion. The suppression order should be reversed.

VII. ARGUMENT

THE DISTRICT COURT ERRED WHEN IT SUPPRESSED THE CHILD PORNOGRAPHY EVIDENCE FOUND ON THE DEFENDANT'S LAPTOP COMPUTER.

A. Standard of Review

This Court reviews de novo the district court's determination that the warrantless search of the defendant's laptop was not a valid border search. *United States v. Cardona*, 769 F.2d 625, 628 (9th Cir. 1985).

B. Argument

1. Border Search Exception - Generally

Routine searches of travelers and their belongings at an international border “are not subject to any requirement of reasonable suspicion, probable cause or warrant” *Montoya de Hernandez*, 473 U.S. at 538; *see Arnold*, 523 F.3d at 945-946 (Fourth Amendment does not bar suspicionless search of contents of laptop computer at the border). Customs agents have been given the “broad authority to search upon entry into the United States vehicles and persons, *as well as personal effects*, where they suspect the presence of merchandise subject to duty or unlawfully imported into

the United States.” *United States v. Alfonso*, 759 F.2d 728, 733 (9th Cir. 1985) (citing 19 U.S.C. § 482) (emphasis added).⁸

The authority of the United States to search the baggage of arriving international travelers is based on its inherent sovereign authority to protect its territorial integrity. By reason of that authority, it is entitled to require that whoever seeks entry must establish the right to enter and to bring into the country whatever he may carry.

Torres v. Puerto Rico, 442 U.S. 465, 472-73 (1979). “[T]ravelers entering the country may be required to identify themselves, show their entitlement to come in, *and identify their belongings as lawfully admissible*. *Alfonso*, 759 F.2d at 733 (citing *Carroll v. United States*, 267 U.S. 132, 154 (1925)) (emphasis added).

[I]t is “axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity.” . . . The government has an overriding interest in securing the safety of its citizens and to do this it must seek to prevent “the introduction of contraband into this country.”

United States v. Ickes, 393 F.3d 501, 506 (4th Cir. 2005) (internal citations omitted).

The Supreme Court has stated that “[t]he Government’s interest in preventing the

⁸ The United States Customs Service was transferred to the Department of Homeland Security (DHS) in 2003, *see* 6 U.S.C. §§ 203, 211; at that time, customs inspectional functions became part of U.S. Customs and Border Protection (CBP) and customs investigative functions became part of U.S. Immigration and Customs Enforcement (ICE). For ease of terminology, the government is employing the general term “customs” in this brief, which applies to both CBP and ICE, who possess similar border search authority.

entry of unwanted persons and effects is at its zenith at the international border.” *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). “The primary purpose of a border search is to seize contraband property sought to be brought into the country.” *Alfonso*, 759 F.2d at 733 (citing *Alexander v. United States*, 362 F.2d 379, 382 (9th Cir. 1966)).

In addition to cases, there is a long list of statutes and regulations granting Customs the authority to conduct searches at the border.⁹ Customs has statutory authority to conduct “border searches” in order to search and examine any vehicle or person for merchandise that might be introduced into the United States in any manner contrary to law. 19 U.S.C. §§ 482, 1581. This authority includes the examination of potentially obscene materials. 19 U.S.C. § 1305. “Merchandise” is not to be delivered from the custody of Customs until it has been inspected, appraised, or examined, and found to have complied with the laws of the United States. 19 U.S.C.

⁹ See 19 U.S.C. § 1496 (authorizing customs officials to search the baggage of persons entering the country); 19 C.F.R. § 162.6 (authorizing customs officials to inspect and search all persons, baggage, and merchandise arriving from foreign countries); 19 U.S.C. § 1499(a) (authorizing customs agents to examine and detain imported merchandise); 19 U.S.C. § 1582 (detain and search “all persons coming into the United States from foreign countries.”); 19 U.S.C. § 1595a(c)(3) (authorizing customs officials to detain merchandise introduced contrary to law); 50 App. U.S.C. § 2411(a)(2)(A) (authorizing customs officials to seize and detain goods at ports of entry in the enforcement of war and national defense); 22 U.S.C. § 464 (authorizing customs agents to detain armed vessels and any property found thereon).

§ 1499(a)(1).¹⁰ In the course of conducting such examination, property remains in the custody of Customs, and may be tested off-site by private testing laboratories or by Customs laboratories until “cleared” by Customs. 19 U.S.C. §§ 1499(a)(2)(B) and (b)(1-3). Not only do these statutes vest Customs with broad border search authority concerning specific items, there is a “long-standing practice of seizing goods at the border even when the type of good is not specified in the statute.” *Ickes*, 393 F.3d at 504.

Border searches by their very nature are reasonable under the Fourth Amendment, and require neither a warrant, probable cause, nor articulable suspicion. *Montoya de Hernandez*, 473 U.S. at 538; *United States v. Ramsey*, 431 U.S. 606, 616-18 (1977). “A greater interest on the side of the government at the border is coupled with a lesser interest on the side of the potential entrant. Since ‘a port of entry is not a traveler’s home,’ his expectation of privacy there is substantially lessened.” *Ickes*,

¹⁰After goods are presented for examination, Customs generally has five days, excluding weekends and holidays, in which to either release or detain those goods. 19 U.S.C. § 1499(c)(1). If the goods are not released within those five days, they are deemed detained. *Id.* Customs must “make a final determination with respect to the admissibility of detained merchandise” within thirty days after the merchandise is presented for examination. 19 U.S.C. § 1499(c)(5)(A). Failure to make a final determination within thirty days is “treated as a decision . . . to exclude the merchandise for purposes of [19 U.S.C. § 1514(a)(4)]. . . .” *Id.*

393 F.3d at 506 (citing *United States v. Thirty Seven Photographs*, 402 U.S. 363, 376 (1971)).

These concerns have only increased over time, “heightened by the veritable national crisis in law enforcement caused by [the] smuggling of illicit narcotics” *Montoya De Hernandez*, 473 U.S. at 538 (citing *United States v. Mendenhall*, 446 U.S. 544, 561 (1980)) (Powell, J., concurring). Even more recently, the Seventh Circuit noted that “the events of September 11, 2001, only emphasize the heightened need to conduct searches” at our borders. *United States v. Yang*, 286 F.3d 940, 944 n. 1 (7th Cir. 2002). In addition, “[a] border search need not take place at the actual border. Because of the nature of international travel and transportation, courts have held that border searches may be conducted at places considered the ‘functional equivalent’ of the border.” *Cardona*, 769 F.2d at 628 (citing *Almeida-Sanchez v. United States*, 413 U.S. 266, 273 (1973)).

Unlike searches at the border or functional equivalent of the border, “[t]he ‘extended border search’ doctrine has been applied to entry border searches conducted some time after the border was crossed.” *Id.* (citing *United States v. Caicedo-Guarnizo*, 723 F.2d 1420, 1422 (9th Cir. 1984)). Reasonable suspicion is required for “extended border searches,” which “occur after the actual entry has been effected” and “away from the border where entry is not apparent.” *Guzman-Padilla*, 2009 WL

2182818, at *4-*5. Thus, the legal analysis required of a “border” search and one conducted at the “functional equivalent” of the border is the same, requiring no warrant, probable cause, or even articulable suspicion; however, an “extended border search” requires reasonable suspicion.

This Court has admitted difficulty in distinguishing between an extended border search requiring reasonable suspicion and a search at the functional equivalent of the border, which does not require reasonable suspicion. *See United States v. Whiting*, 781 F.2d 692, 695 (9th Cir. 1986) (noting doctrines are “often blurred”); *Cardona*, 769 F.2d at 628 (“We have recently recognized the difficulty of making sharp distinctions between searches at the functional equivalent of the border and extended border searches.”); *Alfonso*, 759 F.2d at 734 (“[T]he instant case illustrates the difficulty of making sharp distinctions in this area.”). “[T]ime and place are relevant, since the level of suspicion for extended border searches is stricter than the standard for ordinary border searches. Extended border searches occur *after the actual entry has been effected* and intrude more on an individual’s normal expectation of privacy.” *Alfonso*, 759 F.2d at 734 (emphasis added). Although “time and place” are relevant factors in determining whether a search is a “border search” or an “extended border search,” these factors are not dispositive. *Id.*

Searches of laptops may occur during a border search, without reasonable suspicion. *Arnold*, 523 F.3d at 946 (“[W]e are satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border.”) Thus, law enforcement possesses broader authority to search computers under the border search exception than in those situations where a warrant is required. *Compare Arnold*, 523 F.3d at 946, 948, *with United States v. Payton*, No. 07-10567, 2009 WL 2151348, at *5 (9th Cir. July 21, 2009) (within the context of a search based on a warrant, due to the high storage capacity of computers, search warrant must explicitly authorize the search of computers).

2. The Search of The Defendant’s Laptop Was A Border Search

The search of the defendant’s laptop by Special Agent & Computer Forensic Examiner John Owen at an ICE computer forensics lab in Tucson was a border search, even though it occurred a distance from the border. When the defendant crossed the border and arrived at the Lukeville POE, Customs clearly had authority to search his laptop (and other belongings) without a warrant or any degree of suspicion. *Flores-Montano*, 541 U.S. at 152–53; *Arnold*, 523 F.3d at 946. The laptop was detained at the border and was still in Customs’ custody when searched, having never been cleared. Therefore, the search that occurred in the forensics lab in Tucson was merely

a continuation of the original border search that began at the Lukeville POE and did not implicate any heightened expectation of privacy.

This Court has given law enforcement great latitude in subsequently searching material that it has lawfully seized and searched, when the item remains in the uninterrupted custody of law enforcement. *See United States v. Burnette*, 698 F.2d 1038, 1049-50 (9th Cir. 1983) (defendant's purse cursorily searched incident to arrest and more thoroughly searched at police station; "once an item in an individual's possession has been lawfully seized and searched, subsequent searches of that item, so long as it remains in the legitimate uninterrupted possession of the police, may be conducted without a warrant"; once a suspect's expectation of privacy is reduced or destroyed by the initial search, there is no meaningful invasion of any expectation of privacy in a subsequent search).

Here, the district court conceded that the Cottermans' laptops were properly subject to search at the border. (CR 71; ER 1.) Agent Alvarez conducted a preliminary search analogous to what was done in *Burnette* (CR 58; ER 4), and the defendant's computer remained in continuous Customs custody. Because the initial search of the laptop at the Lukeville POE was lawful, and the laptop was never cleared by Customs and remained in their continuous custody when forensically examined in

Tucson, the defendant had no heightened expectation of privacy that was invaded by the forensic search in Tucson.

When finding that the search here was an “extended border search” rather than a border search, the district court found that “[t]he search could have been done . . . at the border because the technician could have traveled down from Tucson with his laptop computer to do the analysis.” (CR 71; ER 1-2). However, not only did Owen testify that any search at the border would not have yielded the same results as a search he could conduct in his Tucson ICE lab, the district court’s observation is simply irrelevant to the question of whether there was a border search.

In *United States v. Hill*, 459 F.3d 966 (9th Cir. 2006), this Court refused to suppress evidence based on the argument that police could have done a similar on-site search of the suspect’s computer. Hill challenged the specificity of a search warrant that allowed officers to remove any computer media from his home without first determining whether it contained the child pornography for which the agents had probable cause to search. He argued that the police should have brought equipment with them to analyze the material on-site. Affirming the district court’s denial of the motion, this Court rejected the idea that the officers could have brought their own computer, noting the exceptional burdens this would place on law enforcement to have proper equipment available, the potential risk of data corruption in an on-site search,

and the fact that an on-site search could take an extended period of time, substantially interfering with the suspect's Fourth Amendment right to have the intrusion limited as much as possible. *Hill*, 459 F.3d at 974-75.

Similarly, if the district court's ruling is correct that a Customs officer (i.e. CBP and ICE) cannot remove a computer from the border to conduct its forensic examination and continuation of its border search, then the Department of Homeland Security (DHS) would need to ensure computers could be searched at the border. Yet, as this Court observed in *Hill*, it would place an exceptional burden on DHS to require it to place a computer forensics lab (and personnel) at every international border, or to require a computer forensics examiner like Agent Owens to drive down to the POE whenever a computer is detained for a border search. In addition, employing the latter scenario (having an examiner drive down) would not yield the same results. Owens testified that he had specialized computer forensics equipment and software at his Tucson lab, that such software is necessary to search unallocated space on a laptop computer, and that his entire lab is not mobile and cannot easily be transported to the POE or efficiently utilized to search a laptop computer that is being detained there. (CR 55; RT 8/27/08 71-73, 79-80; ER 124-26, 132-33.)

Moreover, forcing law enforcement to comply with artificial time constraints during border searches would be as impractical and imprudent as limits on distance

that an item can travel before being considered an “extended” border search. Owens testified that he “turned around this forensic examination in under 48 hours” and this time frame would be “considered quick” when compared to other computer examinations, where “several days” is “typical.” (CR 55; RT 8/27/08 74; ER 127.) Indeed, if Customs officers could not act fast enough to get a forensics expert (or build the many forensic labs needed to have an expert at every POE), then the Customs officers at the border would need to try to search the laptop on site, even if they were not forensic computer experts. In *Hill*, this Court noted the potential for data corruption in an on-site search. This very real risk is what prompted Agent Riley to decline to try to search the defendant’s laptop at the Lukeville POE and to decline to allow him to help her “access” the computer. She said she had no knowledge of computer forensics; she would have been unable to see some of the files with her “naked eye”; and she was aware of the risk posed if she or the defendant tried to access the computer, including deleting files or “the computer could be booby trapped[.]” (CR 55; RT 8/27/08 38, 50; ER 91, 103.)

A personal computer can easily store millions of pages of information, only a small portion of which may be relevant to an investigation. In many types of cases, including child pornography cases, evidence and contraband are not simply found in neatly organized files in obvious sequence:

Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer. . . . There is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it.

Hill, 459 F.3d at 978. Simply put, examining a computer is complicated and time-consuming. It also may vastly differ from case to case, depending on factors that may not be apparent until the examination is in progress. Thus, highly trained computer examiners must analyze every portion of allocated and unallocated space on the hard drive, using multiple forensic tools.

Reasonableness is the key component when considering limitations placed on border searches and the conduct of law enforcement authorities in effecting them. This Court has held that reasonableness in the context of border searches is “incapable of comprehensive definition or mechanical application The scope of the intrusion, the manner of its conduct, and the justification for its initiation must all be considered in determining whether a search comports with reasonableness.” *United States v. Duncan*, 693 F.2d 971, 977 (9th Cir. 1982) (citing *United States v. Guadalupe-Garza*, 421 F.2d 876, 878 (9th Cir. 1970)) (internal quotation marks omitted).

The magistrate judge here (whose findings the district court adopted) twice noted that DHS acted reasonably in conducting the search of Cotterman's laptop: (1) "It is true that the conduct of the officers was reasonable . . ." (CR 58; ER 8); (2) "We need not reach that question here, where the facts show reasonable diligence and speed in conducting the forensic examination." (CR 58; ER 10.) Thus, the suppression order was not based on the lack of reasonableness in conducting the search; it was based on the erroneous belief that a border search could not take place away from the border and several hours later. This conclusion was wrong. *See Alfonso*, 759 F.2d at 736 ("To be quite clear, we do not view the thirty-six hour delay as dispositive. Courts have upheld border searches one hundred fifty miles from the border and one hundred forty-two hours after a border crossing . . .").

Indeed, regardless of the distance the laptop traveled (whether 100, 170 or 180 miles), or the time the analysis took (48 hours), the forensics search in this case was a lawful border search because it was a continuation of the initial, lawful border search. Not only was the computer forensic search "quick" when compared to a typical forensic search (CR 55; RT 8/27/08 74; ER 127), but the district court's focus on the fact that the laptop was searched "at least two days afer (sic) the Cottermans entered the United States" was misplaced. (CR 58; ER 8.) Although the Cottermans were cleared to enter the United States on April 6, 2009, the laptop in question was

never cleared by Customs and was never out of their custody and control. Thus, the forensic examination of the defendant's laptop was a continuation of the search initiated at the border, and therefore did not implicate any heightened expectation of privacy. It was a lawful border search.

The district court attempted to distinguish several cases involving border searches of computers, noting that those cases involved forensic examinations done at or near the point of entry into the United States: *Arnold*, 523 F.3d 941, *Ickes*, 393 F.3d 501, *United States v. Romm*, 455 F.3d 990 (9th Cir. 2006), and *United States v. Roberts*, 274 F.3d 1007 (5th Cir. 2001). (CR 58; ER 6-8.) However, the magistrate overlooked the central holdings of the cases, which clearly support that the search here was a border search. Moreover, none of those decisions employed the analysis used by the magistrate and district court here.

In *Arnold*, 523 F.3d at 943, this Court found that a lawful border search had been conducted of the defendant's laptop computer at the Los Angeles Airport after arriving on a flight from the Phillippines. While ICE agents did find child pornography on the defendant's computer, it was only after he had been initially detained for several hours. 523 F.3d at 943. That initial detention for several hours was based on a cursory inspection of the defendant's computer which revealed only

a photo of two nude women. *Id.* The border search was upheld, and nothing in *Arnold* states that a search like the one at bar would not constitute a border search.

Although the search of the computer and disks in *Ickes*, 393 F.3d at 503 (cited in *Arnold*), appeared to occur at the border, nothing in the decision supports that the search here was not a border search. 393 F.3d at 503. Indeed, although agents arrested Ickes after seizing a photo album containing child pornography, they then seized a computer and disks. The opinion states that the computer was searched and the CDs “ultimately” were determined to contain child pornography, but it does not discuss the length of time within which these items were searched. The government’s brief in that case states that the computer was preliminarily examined at the Customs “head house” and then forensically examined two to three months after the arrest of the defendant. *United States v. Ickes*, 2004 WL 5200395 (4th Cir. April 2, 2004) (Brief of the United States). The government argued that the forensic search occurring two to three months later was an “extended border search.” Here, of course, the search was completed in 48 hours and the laptop was never seized after arrest (because the defendant was not arrested), but instead was detained to conduct a border search and was never released by Customs. *Ickes* does not support that the search here was not a border search.

In *Romm*, 455 F.3d at 994, Canadian officials denied the defendant entry based upon a review of his computer's internet history, which listed websites related to child pornography. When the defendant arrived at the airport in Seattle, he was greeted by ICE agents who arranged to search his laptop that night, and despite the defendant's repeated denials about having child pornography on his computer, they eventually located about 10 images. *Id.* This search was upheld as a border search. Nothing in that decision states that the search at bar was not a border search.

While the Fifth Circuit in *Roberts* found that there was reasonable suspicion to justify the search of a passenger on an outbound international flight, the six CDs found in the defendant's shaving kit were not examined at all on the day they were seized. 274 F.3d at 1010. The CDs were sent to a forensic agent who examined them, resulting in the defendant's arrest some eleven months later. *Id.* at 1011. The court found that probable cause existed to allow the examination of the CDs. *Id.* at 1017. Finding reasonable suspicion to search the passenger and probable cause to search and seize the passenger's CDs, the court never analyzed whether these searches would be reasonable as border searches or searches at the functional equivalent of the border. Therefore, nothing in *Roberts* states that the search at bar was not a border search.

The magistrate in this case narrowly focused on time and distance and, contrary to precedent, attempted to fashion a hard and fast "time/distance" limit to border

search authority. However, as noted above, the border search here was lawful, because the laptop was detained at the border, it remained in law enforcement custody when searched, and it was not cleared by Customs. *See United States v. Smith*, 629 F.2d 1301, 1304 (9th Cir. 1980) (noting that distance is not important when analyzing border searches because, before being cleared by Customs, the person or item has “not mingled in the normal stream of commerce so as to lessen certainty that the contraband had come directly across the border . . .”).

3. Alternatively, the Search of The Defendant’s Laptop Was A Search At The “Functional Equivalent of the Border,” Which Also Requires No Reasonable Suspicion

In any event, the search of the defendant’s laptop was lawful as a search at the “functional equivalent” of the border. Some decisions may call a search a “border search,” where others may say it was a border search conducted at the “functional equivalent” of the border, but the legal impact is the same because a border search requires no reasonable suspicion. Even under the time and distance considerations employed by the magistrate and district court, the search was lawful without reasonable suspicion.

When merchandise remains in the custody of Customs to be searched and examined at a location other than the first place of entry into the United States, the

search is not transformed into an “extended border search,” but instead may be considered a search at the functional equivalent of the border. *See United States v. Gallagher*, 557 F.2d 1041, 1044 (4th Cir. 1977) (concluding that a camper searched in Norfolk, Virginia was “physically within the territorial confines of the United States, it never left the official custody of United States Customs Thus, when the camper arrived at Norfolk, it stood at the border for purposes of section 482.”); *United States v. Sheikh*, 654 F.2d 1057, 1069 (5th Cir. 1981), *reversed on other grounds*, *United States v. Zuniga-Salinas*, 952 F.2d 876 (5th Cir. 1992) (upholding a the search that occurred three days after initial entry into the United States and a considerable distance from the initial point of entry (Houston to Dallas) – as a border search, finding that Dallas was the functional equivalent of the border); *United States v. Caminos*, 770 F.2d 361, 364-65 (3d Cir. 1985) (upholding the search of a package eleven days after, and great distance from, its initial entry (New York to Pittsburgh via Chicago), as a search at the functional equivalent of the border); *United States v. Gaviria*, 805 F.2d 1108, 1112 (2d Cir. 1986) (upholding the search eight days later and a considerable distance away from the initial point of entry into the U.S. (Miami to New York) as a search at the functional equivalent of the border; court rejected the defendant’s claim that it was an extended border search, stating that “an extended

border search is a search that is usually conducted after a person or some property has cleared an initial customs checkpoint and has entered the United States”).

The above authority supports that the search of the defendant’s laptop was a search at the functional equivalent of the border. For example, the search in *Gallagher* consumed a total of 9 days and was conducted a distance of 240 miles from the border. In *Sheikh*, the search took 3 days and was conducted a distance of 239 miles. The search took 11 days and was conducted 1253 miles from the border in *Caminos*. It took 8 days to search at a distance of 1290 miles in *Gaviria*.¹¹ Thus, the magistrate and district court erred by focusing on the time the search consumed (48 hours) and the distance the laptop traveled (170 miles). (CR 58, 71; ER 3-16, 1-2.) As the above cases demonstrate, border searches have been conducted after longer periods and much greater distances than what occurred here. Thus, the time and distance cited by the district court did not undermine that a lawful border search or search at the functional equivalent of the border had been conducted, particularly where the laptop was never cleared by Customs.

¹¹ Distances approximate and calculated using mapquest.com. (CR 60; ER 39.)

4. The Search of the Defendant's Laptop Was *Not* An Extended Border Search

As noted earlier, the magistrate and district court wrongly found that the distance from Lukeville to Tucson (“170 miles”) was too far to permit a border search, and that the forensic search of the laptop became an “extended border search,” requiring reasonable suspicion. The magistrate and district court, however, were mistaken about the difference between a border search and an extended border search.

The extended border search doctrine was developed to address circumstances involving a search *initiated* at a time and place removed from the border, often after an initial Customs clearance. In other words, the extended border search typically involved situations where custody of an item was returned by Customs to the item's custodian, or custody was never taken by Customs at the border, and then a subsequent search of that item was conducted after the custodian had made entry into the United States. *See, e.g., United States v. Bennett*, 363 F.3d 947, 951 (9th Cir. 2004) (“Extended border searches . . . occur well after *actual entry*”) (emphasis added); *Alfonso*, 759 F.2d at 734 (“Extended border searches occur *after the actual entry has been effected*”) (emphasis added); *Caicedo-Guarnizo*, 723 F.2d at 1422 (stating “[t]he ‘extended border search’ doctrine . . . permits the Government to

conduct border searches some time *after the border has been crossed*” and further noting the “*delayed nature* of an extended border search”) (emphasis added).

Indeed, an examination of earlier circuit decisions reveals that the primary application of the doctrine was specifically to enable Customs to allow a “break” in custody over the items to be searched as a means of enhancing the government’s enforcement of customs laws. As explained by this Court in *United States v. Espericueta-Reyes*:

[T]he work of customs officials is made far more effective by the identification of accomplices of the carrier bringing contraband into the United States. . . . For that reason, surveillance is often initiated as a person suspected of smuggling contraband crosses the border. A thorough search at the border is often deliberately delayed to avoid forewarning the individuals involved that surveillance is being undertaken. . . . Not all extended border searches are concerned with ‘sweeping in’ accomplices of the carrier of contraband. In some situations, a search is delayed to ‘bolster by further observation a suspicion that is arguably marginal at the time the border crossing was observed. . . . In others, an extended border search is proper because customs officials are first alerted to suspicious circumstances immediately after the vehicle has left the inspection area.

631 F.2d 616, 620 & n.4 (9th Cir. 1980) (internal citations and quotation marks omitted). *See also United States v. Weil*, 432 F.2d 1320, 1323 (9th Cir. 1970) (stating that Customs Officers have the right to search a vehicle where the occupant crossed the border in a different vehicle but then transferred parcels from the border-crossing

vehicle to the current vehicle); *Alexander v. United States*, 362 F.2d 379, 382 (9th Cir. 1966) (“It requires no discourse to convince that the work of Customs officials is made more effective by identification of the smugglers who bring in the contraband. To that end, it is not always advisable to make the search in the immediate vicinity of the point of border crossing.”); accord *United States v. Bilir*, 592 F.2d 735, 740 & n.9 (4th Cir. 1979) (“Much more commonly, the search away from the border results from deliberate delay by customs officers who have observed an actual border crossing by known suspects but who then follow and only conduct their search at some distance from the border despite repeated intervening opportunities.”).

“Extended border” searches are thought to be more intrusive on an individual’s legitimate expectation of privacy than searches at the border because, “unlike routine border searches, an extended border search may stigmatize the individual searched, is unexpected, and involves greater invasion of privacy” *See Caminos*, 770 F.2d at 364 (citing *United States v. Richards*, 638 F.2d 765, 772 n.4 (5th Cir. 1981)). Once custody of an item has been returned by Customs (or Customs elects not to take custody of a particular item for a search), an individual reasonably would expect that the government’s need and ability to search that item has extinguished. Thus, conducting a subsequent search of that same item infringes on the custodian’s recently-restored privacy interests in that item. *See Espericueta-Reyes*, 631 F.2d at

621 (“[P]rivacy interests protected by the Fourth Amendment play a more significant role after the traveler leaves the border itself.”). Accordingly, such searches must be justified by “reasonable suspicion” that the subject of the search was involved in criminal activity. *Cardona*, 769 F.2d at 628-29; *Alfonso*, 759 F.2d at 734.

The same restoration of privacy interests does not occur where – as was the case here – custody of the item is never returned to the individual custodian. As stated earlier, when the defendant crossed the border and arrived at the Lukeville POE, the government could search his laptop (and other belongings) without warrant or any degree of suspicion. *See Flores-Montano*, 541 U.S. at 152–53; *Arnold*, 523 F.3d at 946. While in secondary inspection, the defendant’s laptop was detained by Customs pursuant to its constitutional border search authority, and was not returned back to the defendant or otherwise cleared through Customs at any point between this time and the forensic examination conducted at ICE’s Tucson Office. Again, the forensic examination in Tucson was a continuation of the search begun at the Lukeville POE, and without any break in custody. *Cf. Espericueta-Reyes*, 631 F.2d at 619 n.2 (treating two separate searches as part of a single search, because the circumstances made it impractical to continue the search that had begun). Therefore, nothing occurred during this temporal and spatial interval – on which the district court relies – to have restored the defendant’s privacy interests, and if no suspicion was required

at the border to search his laptop, then no suspicion was required to continue that search in Tucson. *See Caminos*, 770 F.2d at 365 (“[T]he ‘reasonable suspicion’ showing is justified where the later search is unexpected, or entails a greater intrusion on expectations of privacy. Where a package is searched while still under customs bond and prior to its delivery to the addressee, these concerns are not implicated.”)

The cases cited in the magistrate’s R&R are all distinguishable. (CR 58; ER 9.) In *Alfonso*, a ship was initially inspected by five Customs inspectors, allowed to enter United States waters and thereafter was placed under surveillance for the next thirty-six hours as it sat anchored off the coast. 759 F.2d at 731-32. During the ensuing thirty-six hours of surveillance, law enforcement observed various individuals coming and going, including the following: one person identified with the boat donning scuba gear and swimming in the direction of the boat; two men leaving the ship carrying a box who were stopped in their vehicle a short while later, resulting in the seizure of forty pounds of cocaine; and two women leaving the ship with duffel bags who were stopped a short while later and seventeen pounds of cocaine was seized. *Id.* at 732. Due to the lapse of thirty-six hours between when the ship was first inspected and allowed to enter the United States, this Court held that the subsequent search had to be analyzed as an “extended border search.” *Id.* at 734. This Court stated that

“[e]xtended border searches occur *after the actual entry has been effected* and intrude more on an individual’s normal expectation of privacy.” *Id.* at 734 (emphasis added).

This case is factually distinguishable from *Alfonso*. In *Alfonso*, after five inspectors left the ship, it had cleared Customs and entered the country. The ship was allowed to remain docked at the Los Angeles Harbor and its occupants were allowed to leave the ship and travel around the mainland, thereby entering the stream of commerce away from the border. The ship was not detained, its occupants were not quarantined inside and its contents were not sealed. In this case, the defendant’s laptop was not cleared by Customs; therefore, it was not allowed to enter the country. It was detained by Customs for purposes of conducting a border search, which *Arnold* permits of laptop computers.

The other “extended border search” cases cited by the lower court are also distinguishable. (CR 58; ER 9-10.); *See Whiting*, 781 F.2d at 696 (search of packages at post office destined for Switzerland analyzed under extended border search because post office in question was far removed from border and packages would have gone through two domestic post offices before leaving the country); *Bilir*, 592 F.2d 735 (ship allowed to enter United States at Savannah, Jacksonville, Galveston, New Orleans, and Baltimore, and vehicle associated with occupants were under surveillance for most of the time they were traveling; extended border search analysis

applied); *United States v. Sahanaja*, 430 F.3d 1049, 1054 (9th Cir. 2005) (search of package by ICE at post office, where it had been mailed to California from Canada nine days after its attempted delivery by postal carrier, analyzed as extended border search); *Cardona*, 769 F.2d at 628-29 (search of Federal Express package being mailed from California to Colombia 24 hours before the package was to leave the country and 3,000 miles away from the border it was to cross was analyzed as an extended border search).

This Court distinguished *Cardona* recently, calling the continued vitality of *Cardona* into question. In *United States v. Abbouchi*, 502 F.3d 850, 855 (9th Cir. 2007), this Court upheld the search of a package mailed from California to Lebanon at a mailing hub in Louisville, Kentucky, as a search occurring at the functional equivalent of the border requiring no reasonable suspicion. The Court declined to analyze the case as an “extended border search ” (although the package might have been airlifted to another city in the United States before leaving the country) and distinguished the case from *Cardona* by noting that it was searched “at the last practicable opportunity for inspection.” *Id.* at 853, 855. Finding Louisville to be the functional equivalent of the border, this Court stated:

Even if the airplanes briefly stop at another hub or airport to refuel or redistribute cargo before departing our country, it is unreasonable to require customs officials to wait until that last domestic stop to unload

the packages from the airplane, reopen the sealed containers, and conduct an inspection before allowing the airplane to proceed to its international destination. Certainly, the search at the Louisville hub represents no greater intrusion on Abbouchi's privacy interests than a search at the last possible moment before the package's departure from the United States.

Id. at 856; *see also United States v. Bareno-Burgos*, 739 F.Supp. 772, 779 (E.D.N.Y. 1990) (distinguishing *Cardona* and noting that “neither the Supreme Court nor the Second Circuit has focused on time and space in determining whether a search was conducted at the functional equivalent of the border or at an extension thereof. Indeed, . . . *what was more relevant to an extended border search than time and space was the fact that a person or some property has initially cleared Customs and entered the United States.*”) (citation omitted) (emphasis added). *Cardona* also appears to conflict with out-of-circuit precedent, which it never distinguished. *See United States v. Udofot*, 711 F.2d 831, 840 (8th Cir. 1983).

In the case at bar, the district court wrongly determined that the search of the defendant's laptop was an “extended border search” requiring reasonable suspicion, rather than a “border search,” which did not.¹²

¹² Although the defendant's laptop is the focus of this appeal, the government notes that the district court's order requiring the government to return the government-owned copy of Mrs. Cotterman's hard drive to the defendant was also erroneous. The district court imposed relief beyond what was requested by the defendant when it
(continued...)

5. Practical Ramifications of the District Court's Decision

As noted earlier, when discussing this Court's observations in *Hill*, 459 F.3d at 974-975, there are some serious practical difficulties with the district court's ruling. Requiring agents to search laptops and other electronic media at the time and place of entry, when this is not required to conduct a lawful border search, could hamper the government's ability to conduct effective border searches.

First, the government may not be able to comply with the time limits set by the district court. There are simply a limited number of qualified forensic examiners. Despite the best efforts of the government to analyze seized computers quickly, "it often takes considerable time to secure the services of a person with the necessary expertise to conduct the search, and it often takes considerable time for such an expert

¹²(...continued)

ordered the return of the government's copy of Mrs. Cotterman's hard drive (and photocopies of papers found in the Cottermans' vehicle). (CR 58; ER 12-13.) The judge lacked authority to issue a ruling concerning Mrs. Cotterman's computer, when she was not a defendant in this case. The court also ordered the government to give the defendant property that he does not own. In support of its decision, the district court noted that CFE Owen "suggested some vague, speculative ways in which the hard drive could possibly, but apparently not actually, contain probative information." (CR 58; ER 13.) Owen actually testified that Mrs. Cotterman's laptop could contain information relevant at trial in the form of e-mail correspondence and metadata that ties the digital cameras and video – used by the defendant to create visual depictions of the sexual abuse of a minor – to the defendant on certain dates and in certain locations. (CR 55; RT 8/27/08 76-77; ER 129-30.)

to analyze a storage device containing many gigabytes of data” *United States v. Mitchell*, 2007 WL 2915889, *11 (S.D. Ga. 2007). For these additional reasons, specifying time periods for the completion of forensic examinations is unreasonable.

Second, as noted earlier, if government officials are required to conduct all routine border searches of computers at the physical border and within a short period of time, the government would be faced with an impossible choice between equipping every POE with trained computer specialists and equipment on the one hand, and limiting its border searches of computers to cursory reviews of easily retrieved data by officers with limited training on the other. Because the former option is costly and resource-intensive, it seems likely that the government would be forced into the latter option and would therefore have to limit the scope of computer border searches in most cases.

Third, the government’s inability to conduct a comprehensive forensic review of computers during a routine border search could have a negative impact on criminal and national security cases. Again, Customs has statutory authority to conduct border searches to search for merchandise that might be introduced into the United States in any manner contrary to law. 19 U.S.C. §§ 482, 1581. These concerns have only increased over time, “heightened by the veritable national crisis in law enforcement caused by [the] smuggling of illicit narcotics,” *Montoya De Hernandez*, 473 U.S. at

538, as well as “[t]he events of September 11, 2001.” *Yang*, 286 F.3d at 944 n. 1. Although officers who are not trained in computer forensics would be able to conduct some basic searches of computers at the border, these searches would not reach large swaths of potentially important data that trained specialists could recover in a lab with proper equipment. The testimony of Owens and Riley alluded to these facts. For example, trained forensic examiners can often recover files that the user has deleted from the computer, even though this data would essentially be invisible to most lay people. These deleted files would probably not be retrieved during a cursory search of a computer at the border.

Perhaps more critically, trained forensic analysts who have access to specialized equipment, such as forensic software, can unlock password-protected files and computers in a relatively short period of time, and in some cases can even “break” the encryption on computers that have been encrypted. However, an officer without forensic training and equipment would likely be unable to accomplish this during a brief search of a computer at the border, absent the consent of the computer user. Since comprehensive searches of computers cannot feasibly be conducted on demand at every border crossing because of the resource constraints described above, the geographic and temporal restrictions on border searches imposed by the district court here would essentially preclude the government from searching any of the data on

password-protected or encrypted computers during a routine border search, except in rare cases.

Because the strategies described above – i.e., deleting files, password-protecting computer data, and encryption – can hide computer data from view during a preliminary or cursory search, technology-savvy criminals who use computers in furtherance of their crimes can employ these strategies to protect or conceal those portions of their computers that contain contraband or evidence of criminal activity. Accordingly, under the district court’s rule here, criminals who want to bring contraband into the country on their computers could simply conceal the data in one or more of these ways and thereby frustrate the government’s ability to inspect that information during a routine border search, if the computer could not be sent away from the border to be examined in the absence of reasonable suspicion.

Even if a system was set up that enabled computer forensic experts to travel to any border crossing in a short period of time with the necessary equipment, a group of conspirators could frustrate this system by attempting to bring numerous computers into the country through multiple border crossings simultaneously, thereby overwhelming the capabilities of the assigned analyst and practically ensuring that he could not inspect each computer at each border crossing within the time frame designated by the magistrate here. In a world where the rule in *Cotterman*’s case

became the norm, such techniques could be used to import or export massive quantities of contraband, such as child pornography, stolen personal information (e.g., credit card numbers or social security numbers), information that threatens national security (e.g., engineering plans), and compromised intellectual property, just to name a few examples.

The government respectfully urges this Court to reverse the district court's decision. It is erroneous and would unreasonably limit the government's ability under its border search authority to conduct a forensic search of a computer away from the border, when this is merely a continuation of a search that began at the border, and the computer has not been cleared by Customs and remains in their continuous control. The district court's rule would frustrate the ability of Customs to comply with its statutory authority where, even as in this case, the search was reasonable and fully complied with the Fourth Amendment. The district court's order should be reversed.

VIII. CONCLUSION

For the foregoing reasons, the district court's order suppressing the evidence in this case should be reversed.

JOHN J. TUCHI
United States Attorney
District of Arizona

CHRISTINA M. CABANILLAS
Appellate Chief

/s Carmen F. Corbin

CARMEN F. CORBIN
Assistant U.S. Attorney

IX. STATEMENT OF RELATED CASES

To the knowledge of counsel, there are no related cases pending.

X. CERTIFICATE OF COMPLIANCE PURSUANT TO FED. R. APP. P. 32(a)(7)(C) AND CIRCUIT RULE 32-1 FOR CASE NO. 09-10139

I certify that: (check appropriate option(s))

 X 1. Pursuant to Fed. R. App. P. 32(a)(7)(C) and Ninth Circuit Rule 32-1, the attached opening/answering/reply/cross-appeal brief is

- ☒ Proportionately spaced, has a typeface of 14 points or more and contains 10,585 words (opening, answering, and the second and third briefs filed in cross-appeals must not exceed 14,000 words; reply briefs must not exceed 7,000 words), or is
- ☐ Monospaced, has 10.5 or fewer characters per inch and contains _____ words or _____ lines of text (opening, answering, and the second and third briefs filed in cross-appeals must not exceed 14,000 words or 1,300 lines of text; reply briefs must not exceed 7,000 words or 650 lines of text).

 2. The attached brief is **not** subject to the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) because

- ☐ This brief complies with Fed. R. App. P. 32(a)(1)-(7) and is a principal brief of no more than 30 pages or a reply brief of no more than 15 pages;
- ☐ This brief complies with a page or size-volume limitation established by separate court order dated _____ and is
- ☐ Proportionately spaced, has a typeface of 14 points or more and contains _____ words, or is
- ☐ Monospaced, has 10.5 or fewer characters per inch and contains _____ pages or _____ words or _____ lines of text.

August 31, 2009

Date

/s/ Carmen F. Corbin

Assistant U.S. Attorney

XI. CERTIFICATE OF SERVICE

I hereby certify that on this 31st day of August, 2009, I electronically filed the Opening Brief with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system. Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

/s/ Carmen F. Corbin

Assistant U.S. Attorney

CMC/sr